PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference PCT	FOR FURTHER ACTION	See Form PCT/IPEA/416
International application No. PCT/EP2004/003177	International filing date *(day/month/year)* 25.03.2004	Priority date *(day/month/year)* 04.04.2003
International Patent Classification (IPC) or national classification and IPC G11B20/00, G06F17/30, G06F7/00, G06F12/00, G06F3/06		
Applicant SONY DADC AUSTRIA AG ET AL.		

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 97 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:
   a. ☒ *sent to the applicant and to the International Bureau)* a total of 2 sheets, as follows:
      ☒ sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).
      ☐ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.
   b. ☐ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing and/or tables related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).

4. This report contains indications relating to the following items:

☒	Box No. I	Basis of the opinion
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

Date of submission of the demand	Date of completion of this report
11.10.2004	01.07.2005
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Barel-Faucheux, C Telephone No. +49 89 2399-2516

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/EP2004/003177

Box No. I Basis of the report

1. With regard to the **language**, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

   ☐ This report is based on translations from the original language into the following language , which is the language of a translation furnished for the purposes of:
   - ☐ international search (under Rules 12.3 and 23.1(b))
   - ☐ publication of the international application (under Rule 12.4)
   - ☐ international preliminary examination (under Rules 55.2 and/or 55.3)

2. With regard to the **elements*** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

Description, Pages

1, 3-13	as originally filed
2, 2a	received on 27.01.2005 with letter of 25.01.2005

Claims, Numbers

1-15	as originally filed

Drawings, Sheets

1/3-3/3	as originally filed

☐ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing

3. ☐ The amendments have resulted in the cancellation of:
   - ☐ the description, pages
   - ☐ the claims, Nos.
   - ☐ the drawings, sheets/figs
   - ☐ the sequence listing *(specify)*:
   - ☐ any table(s) related to sequence listing *(specify)*:

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).
   - ☐ the description, pages
   - ☐ the claims, Nos.
   - ☐ the drawings, sheets/figs
   - ☐ the sequence listing *(specify)*:
   - ☐ any table(s) related to sequence listing *(specify)*:

* *If item 4 applies, some or all of these sheets may be marked "superseded."*

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-15
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-15
Industrial applicability (IA)	Yes:	Claims	1-15
	No:	Claims	

2. Citations and explanations (Rule 70.7):

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Reference is made to the following documents:

D1: EP-A-0 930 615 (FUJITSU LTD) 21 July 1999 (1999-07-21)
D2: US 2002/174102 A1 (KYLER DANIEL B) 21 November 2002 (2002-11-21)
D3: US-B1-6 523 102 (ALVAREZ II MANUEL J ET AL) 18 February 2003 (2003-02-18)
D4: EP-A-1 081 697 (SONY CORP) 7 March 2001 (2001-03-07)

1. The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claims 1 to 15 does not involve an inventive step in the sense of Article 33(3) PCT.

1.1. Document **D1**, which is considered to represent the most relevant state of the art, discloses (cf. column 4, line 47, to column 5, line 33; column 5, line 45, to column 7, line 29; figures 1, 3 and 4) a

method to protect content within protected data areas on a target optical record carrier against unauthorized reading and/or copying with a computer, by the steps of :
- determining whether a target optical record carrier or a non-target optical record carrier is inserted into a drive of the computer, and
- in case a target optical record carrier is inserted into the drive of the computer
  - the Disk Definition Structure (DDS) information can not be obtained so that access to the user area for reading or writing is inhibited.

from which the subject-matter of claim 1 differs in that
- in case a target optical record carrier is inserted into the drive of the computer,
  - modifying read requests to the protected data areas so that no data is read or the read data is useless, and/or
  - modifying write commands in respect to the data within the protected data areas to a recordable record carrier or other storage so that the written data is useless.

1.2. The problem to be solved here may therefore be regarded as providing a means to inhibit access to the read data or to prevent writing of data to a recordable record carrier (see application on page 2, lines 10-13). This problem is known from **D1** (column 5, line 56, to column 6, line 11).

1.3. The solution proposed in claim 1 of the present application cannot be considered as involving an inventive step (Article 33(3) PCT) for the following reasons.

In **D1**, when an operator requests a read or a write to the disk, a SCSI command is transmitted by the computer to the ODC to start the writing or reading of data (column 5, lines 16-22).

D2 discloses a filter driver which operates in a kernel mode, i.e. by control of the core of the Operating System (OS). For example, this core of the OS would launch the filter driver in case a target optical record carrier is inserted into the drive of the computer. The filter driver detects files that are attempted to be written to the server and according to the type of the file, the writing of the file to the recording medium will be blocked or a predetermined policy will be executed (column 1, lines 38-60; column 3, lines 27-48; Figures 1 and 3).

The person skilled in the art will use, without exercising inventive activity, a filter driver similar to the one disclosed in **D2** in order to intercept the SCSI commands for writing or reading of data from **D1** and then modify this read requests to the protected data areas so that no data is read or the read data is useless, and/or modify write commands in respect to the data within the protected data areas to a recordable record carrier or other storage so that the written data is useless, by giving for example erroneous address information from the modified DDS to the read requests or write commands.

1.4. The subject-matter of claim 1 does therefore not involve an inventive step.

1.5. The additional feature of claim 2 with regards to claim 1 to which it refers is that the modifying of read requests and/or write commands is performed only in case no authentication is available. In **D1**, the modifying of DDS information is performed only in the case the security flag is set, ie. in case no authentication is available (column 8, lines 18-50; Figure 6). So claim 2 is not inventive either.

1.6. The additional feature of claim 3 with respect to claims 1 or 2 to which it refers is that the determining and modifying steps are performed by routines implemented into a drive control layer within the computer. Using routines is known from **D2** also, so claim 3 is not inventive.

1.7. The additional feature of claim 4 with respect to claim 3 to which it refers is that the routines replace a dispatch routine and a completion routine, and have the functionality to perform the determining and modifying steps and to call the replaced dispatch and completion routines for their execution based on the original or modified read requests and/or write commands.

However read or write requests with dispatch and completion routine are known by the person skilled in the art (see **D3** : column 41, lines 5-25). Thus modifying read requests and/or write commands as in the application will yield to the modification or replacement of dispatch routine and completion routine without inventive step. Thus claim 3 is not inventive.

1.8. The additional feature of claim 5 with respect to claim 3 or 4 to which it refers is that the routines are implemented by a driver that gets installed by an executable that gets automatically started when a target optical record carrier is inserted into the drive.
This is known from **D2** (column 3, lines 27-37 : "kernel mode"), thus claim 5 is not inventive either.

1.9. The additional feature of claim 6 with respect to claim 5 to which it refers is that the driver
- gets automatically loaded after each start of the computer and/or
- does not comprise an unload routine and/or
- changes its name randomly, and/or
- comprises filetimes that are set randomly, and/or
- comprises code that is changed randomly, and/or
- is installed multiple times, but is only one time active, and/or
- can be installed by installation programs spread all over the computer's system.

This is just a matter of design in order to get the security driver protected against

destruction or blocking. (It uses strategies similar to those used by virus on computer)

Thus claim 6 is not inventive.

1.10. The additional feature of claim 7 with respect to claims 5 or 6 to which it refers is that the driver comprises a communication interface to allow an exchange of control data and/or authentication data.

In **D1**, there is also a communication interface to allow an exchange of control data and/or authentication data (Figure 1; column 4, lines 47 to 51).

1.11. The additional feature of claim 8 with respect to the claims to which it refers is that a target optical record carrier is distinguished from a non-target optical record carrier by evaluating
- a predetermined session of the optical record carrier in respect to special modifications, and/or
- at least one of the tables of contents of the optical record carrier in respect to special entries, and/or
- a predetermined session of the optical record carrier in respect to special subcode modifications, and/or
- predetermined data stored on the optical record carrier in respect to a watermark.

1.11.1. First of all, the application does not meet the requirements of Article 84 EPC, because claim 8 is not clear :
what is a **session** of the optical record carrier ? this is not clear neither from the description, nor from the claims.(see application : page 1, line 35, to page 2, line 8; page 5, lines 23-24; page 5, lines 27-28; page 9, lines 35 and 37)

1.11.2. Secondly, it is to be noted that identifying target optical record carrier by a watermark or an entry in one of the TOC is known by the person skilled in the art (see **D4:** column 3, line 53, to column 8, line 1; Figures 1, 2).

1.12. The additional feature of claim 9 with respect to anyone of the preceding claims to which it refers is that the protected data area is identified on basis of :

- a sector type, and/or
- a range of sectors, and/or
- sectors that are subject of specific read sequences.

Direct ways of defining a protected data area would be by sector type, or ranges, or files (ie. sectors that are subject of specific read sequences) without inventive step.

So claim 9 is not inventive.

1.13. The additional feature of claim 10 with respect to the preceding claims to which it refers is that a protected data area is defined by
- at least one predetermined area, and/or
- data stored on the optical record carrier itself.

The person skilled in the art would define a protected data area by at least one predetermined area or data stored on the optical record carrier without inventive step (see for example **D4** where the protected data area is indicated by data stored on the carrier in the form of a watermark : Figure 3).

So claim 10 is not inventive.

1.14. The additional feature of claim 11 with respect to the claims to which it refers is that the modifying of read requests so that the read data is useless, and/or the modifying of write commands so that the written data is useless comprises
a) to abort a corresponding IO Request and/or IO Command with an error and/or
b) to complete the corresponding I/O Request and/or IO Command, but without processing the actual request and/or command, and/or
c) to modify the respective data so that it is useless.

Schemes a) and b) are known from **D2** (column 3, lines 38-42; Figure 1 : steps 104, 105), whereas step c) is known from **D1** (erroneous DDS information). So claim 11 is not inventive.

1.15. According to points 1.1. to 1.14 are claims 12, 13, 14 and 15, relating to respectively

a computer program product, a computer readable storage means, and an optical record carrier, not inventive.

session of the optical record carrier, might be provided in a computer accessible manner in a second session of the optical record carrier. Alternatively, the second session might comprise a link to a content server to provide a computer access. Such a content server might also comprise added value, e.g. music clips or bonus material related to the information content on the optical record carrier. The access to the content stored in the second session and/or to the content server might be provided through an executable file that automatically starts after the copy protected optical record carrier is inserted into the computer drive.

Further, EP 0 930 615 A2 discloses a data storage device and control method therefore. It is disclosed that the management information of a recording medium is altered by a special controller during writing. When trying to access the recording medium first a dedicated controller has to restore the converted management information so that it can be used. Such a restoring is only performed when a first identifier that is recorded on the memory medium and a second identifier that is recorded in the data storage device match. In case no restoring is performed, the reading and writing of data from and to the recording medium is impossible, since the management information is not available. The special and/or dedicated controllers employ firmware to embody the proposed method.

In view of the above, it is the object underlying the present invention to provide an improved system to protect content within protected data areas on a target optical record carrier against unauthorized reading and/or copying with a computer.

According to the present invention, this object is solved by a method to protect content within protected data areas on a target optical record carrier against unauthorized reading and/or copying with a computer as defined in independent claim 1. Preferred embodiments of the method according to the present invention are defined in the respective dependent claims. A computer program product according to the present invention is defined in claim 12, a computer readable storage means according to the present invention is defined in claim 13, and an optical record carrier according to the present invention is defined in claim 14.

The method to protect content within protected data areas on a target optical record carrier against unauthorized reading and/or copying with a computer according to the present invention comprises the steps of

- determining whether a target optical record carrier or a non target optical record carrier is inserted into a drive of the computer, and
- in case a target optical record carrier is inserted into the drive of the computer
  - modifying read requests to the protected data areas so that no data is read or the read data is useless, and/or
  - modifying write commands in respect to the data within the protected data areas to a recordable record carrier or other storage so that the written data is useless.